

LINEAR CONGRUENCES IN TWO VARIABLES

Theorem 1: The system of linear congruences

$$\begin{cases} ax + by \equiv r \pmod{n} \\ cx + dy \equiv s \pmod{n} \end{cases}$$

has a unique solution whenever

$$(ad - bc, n) = 1$$

· **Theorem 2:** The system of linear congruences

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

has a solution if only if $a \equiv b \pmod{(m_1, m_2)}$.

If this condition is satisfied, then the system has only one solution $\pmod{[m_1, m_2]}$.

Example 1: $x \equiv 2 \pmod{4}$

Since $(4, 6) = 2$ and $2 \equiv 4 \pmod{2}$ then the system has a unique solution $\pmod{[4, 6]} = 12$.

$$\bullet \quad x \equiv 2 \pmod{4}$$

$$\Rightarrow 4 \mid (x - 2)$$

By definition of Congruence

$$\Rightarrow x - 2 = 4m, m \in \mathbb{Z}$$

By definition of Divisibility

$$\Rightarrow x - 2 + 2 = 4m + 2$$

Add 2 to both sides of the Equation

$$(2) \quad \Rightarrow x = 4m + 2$$

Since $-2 + 2 = 0$

- $x = 4 \pmod{6}$

$$\Rightarrow 4m + 2 \equiv \pmod{6}$$

*Substitute the value of x from
Equation(2)*

$$\Rightarrow 4m + 2 + -2 \equiv 4 + -2 \pmod{6}$$

*Add -2 to both sides of
Congruence*

$$\Rightarrow 4m \equiv 2 \pmod{6}$$

Since $2 + -2 = 0$ and $4 + -2 = 2$

$$\Rightarrow 4m \equiv 8 \pmod{6}$$

By Congruence Classes Modulo 6

$$2 \equiv 8 \pmod{6}$$

$$\Rightarrow m \equiv 2 \pmod{3}$$

Divide both sides by 4 by Theorem:

$$\text{If } ca \equiv cb \pmod{m}$$

and $(c, m) = 1$, then $a \equiv b \pmod{m}$.

$$\Rightarrow 3|(m - 2)$$

By definition of Congruence

$$\Rightarrow m - 2 = 3p, p \in \mathbb{Z}$$

By definition of Divisibility

$$\Rightarrow m - 2 + 2 = 3p + 2$$

Add 2 to both sides of the Equation

$$(3) \Rightarrow m = 3p + 2$$

Since $-2 + 2 = 0$

- $x = 4m + 2$

Equation(2)

$$\Rightarrow x + 4(3p + 2) + 2$$

*Substitute the value of m
from Equation(3)*

$$\Rightarrow x = (12p + 8) + 2$$

*By Distributive Property for
Multiplication over Addition*

$$\Rightarrow x = (12p + 8) + 2$$

By Associative Property for

Multiplication over Addition

$$\Rightarrow x = 12p + (8 + 2)$$

Since $8 + 2 = 10$

$$\Rightarrow x + -10 = 12p + 10 + -10$$

Add -10 to both sides of

the Equation

$$\Rightarrow x - 10 = 12p$$

LHS: By definition of Subtraction

RHS: Since $10 + -10 = 0$

$$\Rightarrow 12|(x - 10)$$

By definition of Divisibility

$$\Rightarrow 12|(x - 10)$$

By definition of Congruence

Example 2:

$$\left\{ \begin{array}{l} 7x + 3y = 10 \pmod{16} \\ 2x + 5y \equiv 9 \pmod{16} \end{array} \right.$$

Solution:

Euclidean Algorithm:

$$(ad - bc, n) = (7 \cdot 5 - 3 \cdot 2, 16)$$

$$29 = 16(1) + 13$$

$$= (35 - 6, 16)$$

$$16 = 13(1) + 3$$

$$= (29, 16)$$

$$13 = 3(4) + 1$$

$$= \boxed{1}$$

GCD

$$3 = 1(3) + 0$$

Therefore, by Theorem 1, the system of linear congruence

$$\left\{ \begin{array}{l} 7x + 3y \equiv 10 \pmod{16} \\ 2x + 5y \equiv 9 \pmod{16} \end{array} \right. \text{ has a unique solution.}$$

To eliminate variable x from the system,

we have:

$$\begin{array}{rcl}
 \left. \begin{array}{l} [7x + 3y \equiv 10 \pmod{16}] - 2 \\ [2x + 5y \equiv 9 \pmod{16}] \cdot 7 \end{array} \right\} & \rightarrow & \begin{array}{l} 14x + -6y \equiv -20 \pmod{16} \\ 14x + 35y \equiv 43 \pmod{16} \end{array} \\
 (1) & & \boxed{129y \equiv 43 \pmod{16}}
 \end{array}$$

$$\bullet \quad 29y \equiv 43 \pmod{16}$$

From Congruence (1)

$$\Rightarrow 29y \equiv 27 \pmod{16}$$

*By Transitive Property for
Congruence*

$$\Rightarrow 29y \equiv 11 \pmod{16}$$

*By Transitive Property for
Congruence*

$$\Rightarrow 29y \equiv -5 \pmod{16}$$

*By Transitive Property for
Congruence*

$$\Rightarrow 45y \equiv -5 \pmod{16}$$

By Congruence Classes Modulo 16

$$29y \equiv 11 \pmod{16}$$

$$\Rightarrow 9y \equiv -1 \pmod{16}$$

*Divide both sides 5 by Theorem: If
 $ca \equiv cb \pmod{m}$ and $(cm) = 1$,
then $a \equiv b \pmod{m}$*

$$\Rightarrow 9y \equiv 15 \pmod{16}$$

*By Transitive Property For
Congruence*

$$\Rightarrow 3y \equiv 5 \pmod{16}$$

Divide both sides of the congruence

$$\Rightarrow 3y \equiv 21 \pmod{16}$$

$$\Rightarrow y \equiv 7 \pmod{16}$$

To eliminate variable y from the system,

we have:

$$\begin{array}{lcl} \left\{ \begin{array}{l} [7x + 3y \equiv 10 \pmod{16}] \cdot 5 \\ [2x + 5y \equiv 9 \pmod{16}] \cdot 3 \end{array} \right. & \rightarrow & \begin{array}{l} 35x + 15y \equiv 50 \pmod{16} \\ \underline{(6x + 15y \equiv 27 \pmod{10})} \end{array} \\ (2) & & \boxed{29x \equiv 23 \pmod{16}} \end{array}$$

$$\bullet \quad 29x \equiv 23 \pmod{16}$$

$$\Rightarrow 29x \equiv 7 \pmod{16}$$

$$\Rightarrow 45x \equiv 7 \pmod{16}$$

by 3 by Theorem: If $ca \equiv$

$cb \pmod{m}$ and $(cm) = 1,$

then $a \equiv b \pmod{m}$

By Transitive Property for

Congruence

Divide both sides of the Congruence

by 3 by Theorem. If $ca \equiv$

$cb \pmod{m}$ and $(c, m) = 1$

then $a \equiv b \pmod{m}$

From Congruence (2)

By Transitive Property for

Congruence

By Congruence Classes Modulo 16

$$45x \equiv 29x \pmod{16}$$

$$\Rightarrow 61x \equiv 7 \pmod{16}$$

By Congruence Classes Modulo 16

$$61x \equiv 45x \pmod{16}$$

$$\Rightarrow 77x \equiv 7 \pmod{16}$$

By Congruence Classes Modulo 16

$$77x \equiv 61x \pmod{16}$$

$$\Rightarrow 11x \equiv 1 \pmod{16}$$

Divide both sides of the congruence

by 7 by Theorem: If $ca \equiv$

$cb \pmod{m}$ and $(cm) = 1,$

then $a \equiv b \pmod{m}$

$$\Rightarrow -5x \equiv -15 \pmod{16}$$

By Congruence Classes Modulo 16

$$11x \equiv -5x \pmod{16} \text{ and}$$

$$1x \equiv -15x \pmod{16}$$

$$\Rightarrow x \equiv 3 \pmod{16}$$

Divide both sides of the congruence

by -5 by Theorem: If $ca \equiv$

$cb \pmod{m}$ and $(cm) = 1,$

then $a \equiv b \pmod{m}$

Checking:

$$x \equiv 3 \pmod{16}$$

$$y \equiv 7 \pmod{16}$$

- $7x + 3y \equiv 10 \pmod{16}$

$$\Rightarrow 7(3) + 3(7) \equiv 10 \pmod{16}$$

$$\Rightarrow 21 + 21 \equiv 10 \pmod{16}$$

$$\Rightarrow 42 \equiv 10 \pmod{16}$$

$$\bullet \quad 2x + 5y \equiv 9 \pmod{16}$$

$$\Rightarrow 2(3) + 5(7) \equiv 9 \pmod{16}$$

$$\Rightarrow 6 + 35 \equiv 9 \pmod{16}$$

$$\Rightarrow 41 \equiv 9 \pmod{16}$$

Thus, the unique solution to the system of linear congruence with two variables

$$\left\{ \begin{array}{l} 7x + 3y \equiv 10 \pmod{16} \\ 2x + 5y \equiv 9 \pmod{16} \end{array} \right.$$

is

$$x \equiv 3 \pmod{16}$$

$$y \equiv 7 \pmod{16}$$